Constructions of Partial Difference Sets and Relative Difference Sets Using Galois Rings II

Yu Qing Chen, D. K. Ray-Chaudhuri, and Qing Xiang*.

Department of Mathematics, Ohio State University, Columbus, Ohio 43210
*Department of Mathematics, California Institute of Technology, Pasadena, California 91125

Communicated by the Managing Editors
Received June 20, 1995

In a previous paper, [Des., Codes and Cryptogr. 8 (1996), 215–227]; we used Galois rings to construct partial difference sets, relative difference sets and a difference set. In the present paper, we first generalize and improve the construction of partial difference sets in [Des., Codes and Cryptogr. 8 (1996), 215–227]; also we obtain a family of relative difference sets from these partial difference sets. Second, we construct a class of relative difference sets in \((\mathbb{Z}_4)^{2m+1} \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_2)^r\), \(r+s=m, r, s \geq 0\) with respect to a subgroup \((\mathbb{Z}_2)^{m+1}\). These constructions make use of character sums from Galois rings, and relate relative difference sets to Hadamard difference sets.

1. INTRODUCTION

Let \(G\) be a finite group of order \(v\). A \(k\)-element subset \(D\) of \(G\) is called a \((v, k, \lambda, \mu)\)-partial difference set (PDS) in \(G\) if the differences \(d_1d_2^{-1}, d_1, d_2 \in D, d_1 \neq d_2\), represent each nonidentity element in \(D\) exactly \(\lambda\) times and each nonidentity element not contained in \(D\) exactly \(\mu\) times. \(D\) is called abelian if \(G\) is abelian. It is well known that a PDS \(D\) with \(e \notin D\) and \(|d^{-1}: d \in D| = D\) is equivalent to a strongly regular Cayley graph, such a PDS is called regular. The study of partial difference sets is closely related to partial geometries, Schur rings, strongly regular Cayley graphs and two-weight codes. The recent survey of Ma [5] contains very detailed descriptions of these connections.

Assume that \(v = mn\) and that \(G\) contains a normal subgroup \(N\) of order \(n\). A \(k\)-element subset \(R\) of \(G\) is called an \((m, n, k, \lambda)\)-relative difference set (or, in short an \((m, n, k, \lambda)\)-RDS) in \(G\) relative to \(N\) if the differences \(d_1d_2^{-1}, d_1, d_2 \in R, d_1 \neq d_2\), represent each element in \(G\) not in \(N\) exactly \(\lambda\) times and each nonidentity element in \(N\) zero time. If \(G = H \times N\), where \(H\) is...
some subgroup of $G$, then $R$ is called a splitting RDS. We will focus on
$(p^n, p^n, p^n, p^n)$-relative difference sets in this paper, these relative dif-
ference sets have been studied extensively, we refer the reader to the recent

In a previous paper [7], we used Galois rings to construct partial dif-
ference sets, relative difference sets and a difference set. The main idea is as
follows. Given a subgroup of the unit group of a Galois ring, we may view
the orbits of the multiplication action of that subgroup on the Galois ring
as analogues of cyclotomic classes of finite fields, hence they may be used
to construct partial difference sets, relative difference sets, and difference
sets. Instead of calculating cyclotomic numbers, we use additive characters
of the Galois ring to show that the candidate subsets we come up with
have the required “difference” property. Galois rings have attracted a great
deal of attention recently because of their applications in coding theory
[3]. In this paper, we first generalize and improve the construction of par-
tial difference sets in [7]; also we obtain a family of relative difference sets
from these partial difference sets. Second, we construct a class of non-
splitting relative difference sets in $(Z_4)^{2m+1} \oplus (Z_4)^r \oplus (Z_2 \oplus Z_2)^s$, $r + s = m$
, $r, s \geq 0$ with respect to a subgroup $(Z_2)^{2m+1}$.

The following well-known character theoretic characterizations of
abelian partial difference sets and relative difference sets will be used in our
constructions.

**Lemma A.** Let $G$ be an abelian group of order $v$ and $D$ be a subset of $G$
with $\{d^{-1}: d \in D\} = D$. Then $D$ is a $(v, k, \lambda, \mu)$-partial difference set in $G$
if and only if, for any character $\chi$ of $G$,

$$\sum_{d \in D} \chi(d) = \begin{cases} 
k & \text{if } \chi \text{ is principal on } G, \\
\beta \pm \sqrt{\beta^2 + 4\gamma} \over 2 & \text{if } \chi \text{ is nonprincipal on } G,
\end{cases}$$

where $\beta = \lambda - \mu; \gamma = k - \lambda$ if $e \in D$, and $\gamma = k - \mu$ if $e \notin D$.

**Lemma B.** Let $G$ be an abelian group of order $mn$ with a subgroup $N$
of order $n$, and $R$ be a $k$-element subset of $G$. Then $R$ is an $(m, n, k, \lambda)$-relative
difference set in $G$ relative to $N$ if and only if, for any character $\chi$ of $G$,

$$\sum_{r \in R} \chi(r) = \begin{cases} 
k & \text{if } \chi \text{ is principal on } G, \\
\sqrt{k - 2n} & \text{if } \chi \text{ is nonprincipal on } G \text{ but principal on } N, \\
\sqrt{k} & \text{if } \chi \text{ is nonprincipal on } N.
\end{cases}$$
2. GALOIS RINGS OVER \( \mathbb{Z}/p^2\mathbb{Z} \)

For every integer \( t \geq 1 \), let \( F_t \) denote the finite field of order \( p^t \), where \( p \) is a prime. Let \( \mu_t : \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = F_1 \) be the modulo \( p \) reduction map.

We can extend \( \mu_t \) to \( \mathbb{Z}/p^2\mathbb{Z}[x] \) in the natural way. Let \( \Phi(x) \) be a primitive polynomial of degree \( t \) over \( F_p \) and let \( \mu_1(x) = \Phi(x) \) be the homomorphism \( \mu_1 \). There is a unique monic \( \Phi(x) \) whose root \( g \) satisfies \( g^p - 1 = 1 \).

The ring \( \mathbb{Z}/p^2\mathbb{Z}[g] \) is an algebraic extension of \( \mathbb{Z}/p^2\mathbb{Z} \); it is the Galois extension of \( \mathbb{Z}/p^2\mathbb{Z} \) of degree \( t \). This extension \( \mathbb{Z}/p^2\mathbb{Z}[g] \) is called a Galois ring and is denoted by \( \text{GR}(p^2, t) \).

\( \text{GR}(p^2, t) \) is a finite local ring, it has the unique maximal ideal \( \mathfrak{m} = \{0, p, px, px^2, \ldots, px^{t-2}\} \), where \( q = p^t \), the residue class field \( \text{GR}(p^2, t) / \mathfrak{m} \) = \( \mathbb{F}_q \). We can take the Teichmuller system \( T = \{0, 1, g, \ldots, g^{t-2}\} \) as a set of representatives of \( \text{GR}(p^2, t) / \mathfrak{m} \).

Therefore an arbitrary element \( \sum a_i x^i \in \text{GR}(p^2, t) \) is uniquely represented as \( \sum a_i x^i + \sum b_i x^i \), where \( a_i, b_i \in \mathbb{Z}/p^2\mathbb{Z} \). We denote the set of invertible elements of \( \text{GR}(p^2, t) \) by \( \text{GR}(p^2, t)^* \). Every element of \( \text{GR}(p^2, t)^* \) has a unique representation in the form \( g^i(1+px) \), \( 0 \leq i \leq q-2 \), \( x \in T \). \( \text{GR}(p^2, t)^* \) is a multiplicative group of order \( (p^t-1)p^t \) which is a direct product \( H \times \mathcal{U} \), where \( H \) is the cyclic group of order \( p^t-1 \) generated by \( g \), and \( \mathcal{U} \) is the group of principal units of \( \text{GR}(p^2, t) \), that is, elements of the form \( 1 + px \), \( x \in T \). \( \mathcal{U} \) has the structure of an elementary abelian group of order \( p^t \) and is isomorphic to the additive group of \( \mathbb{K} \) via the map \( 1 + px \mapsto x, x \in T \).

For the proof of the above assertions on the structure of \( \text{GR}(p^2, t)^* \) and more detailed description of Galois rings, we refer the reader to MacDonald [6].

For \( x \in K = \{0, 1, g, \ldots, g^{t-2}\} \), we define the trace function from \( K \) to \( F_p \) by \( tr_{s,1}(x) = x + x^p + \ldots + x^{p^{s-1}} \). Let \( s \) be a positive divisor of \( t \). Then there is a unique subfield \( F_p^s \) of \( K \) with \( p^s \) elements, we denote the trace maps from \( K \) to \( F_p^s \) and from \( F_p^s \) to \( F_p \) by \( tr_{s,1} \) and \( tr_{s,1} \) respectively. By transitivity of trace, we have \( tr_{s,1} = tr_{s,1} \circ tr_{s,1} \). The additive characters of \( K \) can be easily described by the trace function.

**Lemma C.** All additive characters \( \chi \) of \( K \) are given by

\[
\chi_s(x) = \zeta_p^{tr_{s,1}(x)}, \quad x \in K
\]

where \( \zeta_p \) is a primitive \( p \)th root of unity.

The Frobenius map \( f \) from \( \text{GR}(p^2, t) \) to \( \text{GR}(p^2, t) \) is the ring automorphism \( f : x_0 + px_1 \mapsto x_0^p + px_1^p, \quad x_0, x_1 \in T \). The Galois group of
GR($p^2$, t) over $\mathbb{Z}/p^2\mathbb{Z}$ is a cyclic group of order $t$ which is generated by $f$. The set of elements of GR($p^2$, t) invariant under $f$ is identical with $\mathbb{Z}/p^2\mathbb{Z}$.

For $x \in$ GR($p^2$, t), we define the trace function from GR($p^2$, t) to $\mathbb{Z}/p^2\mathbb{Z}$ by $T_{x,t}(x) = x + x^2 + \cdots + x^{p^2-1}$. Let $s$ be a positive divisor of $t$. Then there is a unique subring GR($p^2$, s) of GR($p^2$, t) with $p^2s$ elements (see [6]). Let us denote the relative traces from GR($p^2$, t) to GR($p^2$, s) and from GR($p^2$, s) to GR($p^2$, 1) = $\mathbb{Z}/p^2\mathbb{Z}$ by $T_{x,t}$ and $T_{x,1}$ respectively. It is easy to check that $T_{x,t} = T_{x,s}T_{x,1}$ and the diagram

$$
\begin{array}{ccc}
\text{GR($p^2$, t)} & \xrightarrow{T_{x,t}} & K = F_{p^2} \\
& \searrow & \\
\text{GR($p^2$, s)} & \xrightarrow{T_{x,s}} & F_{p^2} \\
& \searrow & \\
\mathbb{Z}/p^2\mathbb{Z} & \xrightarrow{T_{x,1}} & F_p
\end{array}
$$

is commutative, where $T_{x,t}$ and $T_{x,s}$ are the natural homomorphisms from the Galois rings GR($p^2$, t) and GR($p^2$, s) to their residue class fields respectively.

The additive characters of GR($p^2$, t) can also be described by the trace function.

**Lemma D.** All additive character $\lambda_{p^2}$ of GR($p^2$, t) are given as follows

$$
\lambda_{p^2}(x) = \zeta_{p^2}^{T_{x,s}(x)}, \quad x \in \text{GR($p^2$, t)}
$$

where $\zeta_{p^2}$ is a primitive $p^2$th root of unity.

For the proofs of Lemma C and Lemma D, we refer the reader to Yamamoto and Yamada [9].

### 3. PARTIAL DIFFERENCE SETS

In this section, we generalize and improve the construction of partial difference sets in [7]. We will follow the notations used in Section 1 and 2. Considering the subgroup $H$ of GR($p^2$, t)*, we enumerate the cosets of $H$ in GR($p^2$, t)* as, $E_0 = H, E_1 = (1 + p)H, E_2 = (1 + pg)H, \ldots, E_{p^2-1} = (1 + pg^{p^2-2})H$, where $q = p'$. We note that $E_0, E_1, E_2, \ldots, E_{p^2-2}, B\setminus\{0\}$, \{0\} are the orbits of the multiplication action of $H$ on GR($p^2$, t), and $|E_0| = |E_1| = |E_2| = \cdots = |E_{p^2-2}| = q - 1$. 


Let $s$ be a positive divisor of $t$, $s < t$. There exists an element $\overline{0} \neq \overline{g}^n \in K$ such that $tr_{s,t}(\overline{g}^n) = 0$. Let $V = \{ \bar{x} \in K : tr_{s,t}(\overline{g}^n \bar{x}) = 0 \}$. Then $V$ is a $(t/s - 1)$-dimensional $F_{ps}$-subspace of $K$.

Let $V^\perp = \{ \bar{x} \text{ is an additive character of } K; \chi |_{V} = \chi_0 \}$. We claim that $V^\perp = \{ \bar{x}; \bar{h} = \bar{g}^n \bar{x}, \bar{x} \in F^*_{ps} \}$. To see this, one just needs to note that $tr_{s,t}(\bar{x} \bar{g}^n \bar{x}) = \bar{x} tr_{s,t}(\bar{g}^n \bar{x}) = 0$ for all $\bar{x} \in V$, $\bar{x} \in F^*_{ps}$, and $|V^\perp| = |K|/|V| = p^t$.

Define $D = \bigcup_{\bar{x} \in V} E_{\bar{x}}$. Then we have the following theorem.

**Theorem 3.1.** $D$ is an $(n^2, r(n-1), n + r^2 - 3r, r^2 - r)$-PDS in the additive group of $\text{GR}(p^2, t)$ with $n = p^t$, $r = p^{t-1}$; $D \cup (B\setminus \{0\})$ is an $(n^2, r(n-1), n + r^2 - 3r, r^2 - r)$-PDS in the additive group of $\text{GR}(p^2, t)$ with $r_1 = p^{t-1} + 1$.

**Proof.** Let $\lambda$ be an arbitrary additive character of $\text{GR}(p^2, t)$. By Lemma D, we consider the following three cases.

1. $\lambda$ is principal; i.e., $\lambda = \lambda_0$. In this case, $\lambda(D) = |D| = |V|(p^t - 1) = p^t - (p^t - 1)$.

2. $\lambda = \lambda_{p^u}$, $0 \leq u \leq (q - 2)$. In this case, $\lambda$ has order $p$. By the computation in the proof of Theorem 4.1 in [7], we know that $\lambda(E) = -1$. Hence $\lambda(D) = (-1)|V| = -p^{t-1}$.

3. $\lambda = \lambda_{\beta}$, $\beta = (1 + pb)g^u$, where $0 \leq u \leq (q - 2)$, and $b \in \mathcal{F}$. In this case, $\lambda$ has order $p^2$, and

$$
\begin{align*}
\lambda_{\beta}(D) &= \sum_{\bar{x} \in V} \sum_{i=0}^{q-2} \lambda_{\beta}(1 + px(g^i)) \\
&= \sum_{\bar{x} \in V} \sum_{i=0}^{q-2} \sum_{j=0}^{p-1} \sum_{k=0}^{p-1} \chi_{p^2}(1 + px(g^i)) \chi_{p^2}(g^j) \\
&= \sum_{\bar{x} \in V} \sum_{i=0}^{q-2} \sum_{j=0}^{p-1} \sum_{k=0}^{p-1} \chi_{p^2}(1 + px(g^i)) \chi_{p^2}(g^j) \\
&= \sum_{i=0}^{q-2} \sum_{j=0}^{p-1} \sum_{k=0}^{p-1} \chi_{p^2}(1 + px(g^i)) \chi_{p^2}(g^j) \\
&= \sum_{i=0}^{q-2} \chi_{p^2}(1 + px(g^i)) \chi_{p^2}(V).
\end{align*}
$$

By the claim proved before Theorem 3.1, we know that

$$
\chi_{p^2}(V) = \begin{cases} 
|V| & \text{if } \overline{g}^t = \overline{g}^s \bar{x} \text{ for some } \bar{x} \in F^*_{ps}, \\
0 & \text{otherwise}.
\end{cases}
$$
Hence,
\[
\lambda_p(D) = |V| \sum_{x \in F_p^n} \zeta_T(x((1 + pb) g^* x))
\]
\[
= |V| \sum_{x \in F_p^n} \zeta_T(x((1 + pb) g^* x))
\]
\[
= |V| \sum_{x \in F_p^n} \lambda_T(x((1 + pb) g^* x)) + 1.
\]

By the commutative diagram in Section 2, we have
\[
\mu(T_x,((1 + pb) g^*)) = \text{tr}(T_x,((1 + pb) g^*)) = \text{tr}(g^*) = 0.
\]
This shows that \( T_x,((1 + pb) g^*) \) is in the maximal ideal of \( GR(p^2, s) \), hence
\[
\lambda_p(T_x,((1 + pb) g^*)) = \text{tr}(T_x,((1 + pb) g^*)) = \text{tr}(g^*) = 0.
\]

Summing up all these calculations, we have shown that, for any nonprincipal additive character \( \lambda \) of \( GR(p^2, s) \), hence \( \lambda(T_x,((1 + pb) g^*)) \) is either the principal character or a character of order \( p \) of \( GR(p^2, s) \). Let \( T_x,((1 + pb) g^*) = pg^* \in GR(p^2, s) \). By the surjectivity of \( \text{tr}_x \), there exists \( b \in K \) such that \( g^* + \text{tr}_x(g^* b) = 0 \); hence there exists \( b \in GR(p^2, t) \) such that \( T_x,((1 + pb) g^*) = 0 \), i.e., \( \lambda(T_x,((1 + pb) g^*)) \) is the principal character for some \( b \in GR(p^2, t) \). Therefore, we have
\[
\lambda_p(D) = \begin{cases} p^{t-1}(p' - 1) & \text{if } \lambda(T_x,((1 + pb) g^*)) \text{ is the principal character,} \\ -p^{t-1} & \text{if } \lambda(T_x,((1 + pb) g^*)) \text{ is a character of order } p. \end{cases}
\]

For the proof of the second part of the theorem, we note that for any nonprincipal additive character \( \lambda \) of \( GR(p^2, t) \),
\[
\lambda(B \setminus \{0\}) = \begin{cases} 1 & \text{if } \lambda \text{ has order } p^2; \\ p' - 1 & \text{if } \lambda \text{ has order } p. \end{cases}
\]

Then by the above calculations of \( \lambda(D) \) and Lemma A, we see that \( D \cup (B \setminus \{0\}) \) is an \( (n^2, r(n - 1), n + r^2 - 3r, r^2 - r) \)-PDS in the additive group of \( GR(p^2, t) \) with \( r = p^{t-1} \). This completes the proof of the theorem.

Remark. In Theorem 3.1, if we let \( s = 1 \) and choose \( g^* = 1 \) (hence \( p \mid t \)), we obtain Theorem 4.1 in [7]. S. L. Ma informed us that he and K. H. Leung also can get rid of the condition \( p \mid t \) in our previous construction in [7] by using very different method. Here we could generalize our original construction to the case \( t > s > 1, s \mid t \).

We continue to obtain more partial difference sets from the above construction.
Since $V = \{ \bar{x} \in K : \text{tr}_x (\overline{g} \bar{x}) = 0 \}$ is an $F_{p^m}$-subspace of $K$, $D = \bigcup_{i \in \mathbb{Z}} V_i$ is a subgroup of $\text{GR}(p^2, t)^*$. Let $D_0 = D, D_1 = g_1 D, ..., D_{p^m-1} = g_{p^m-1} D$ be the cosets of $D$ in $\text{GR}(p^2, t)^*$, where $g_i \in \mathcal{B}, 1 \leq i \leq p^m - 1$. The character values of $D_i$ can be easily calculated as

$$\lambda_0(D_i) = p^{t-x}(p^t - 1),$$

and

$$\lambda_{p^m}(D_i) = \lambda_{p^m-1}(D_0) = -p^{t-x},$$

and

$$\lambda_{(1 + ph)g^x}(D_i) = \begin{cases} p^{t-x}(p^t - 1) & \text{if } \lambda_{T_x(i (1 + ph)g^x)} \text{ is the principal character}, \\ -p^{t-x} & \text{if } \lambda_{T_x(i (1 + ph)g^x)} \text{ is a character of order } p. \end{cases}$$

for $i = 1, 2, ..., p^m - 1$.

Also, for any fixed character $\lambda_{(1 + ph)g^x}$, we have

$$\sum_{i=0}^{p^m-1} \lambda_{(1 + ph)g^x}(D_i) = \lambda_{(1 + ph)g^x}(\text{GR}(p^2, t)^\mathcal{B}) = 0.$$ 

Let $x = \sum_{i=0}^{p^m-1} \lambda_{(1 + ph)g^x}(D_i) = p^{t-x}$, then the above equation becomes $x(p^{t-x}) - (p^t - x)p^{t-x} = 0$; hence $x = 1$. From this observation we have the following theorem.

**Theorem 3.2.** Let $\mathcal{I} = \{i_1, i_2, ..., i_{l} \} \subseteq \{0, 1, 2, ..., p^m - 1\}$, $1 \leq l \leq p^m$. $D_{i_1} \cup D_{i_2} \cup \cdots \cup D_{i_l}$ is an $(n^2, r, n + r_2 - 3r_2, r_2 - r_3)$-PDS in the additive group of $\text{GR}(p^2, t)$, then

$$\bigcup_{i=1}^{l} D_{i_j} \cup (\mathcal{B} \setminus \{0\})$$

is an $(n^2, r, n + r_3 - 3r_3, r_3 - r_1)$-PDS in the additive group of $\text{GR}(p^2, t)$ with $r_3 = \text{Ip}^{t-x} + 1$.

**Proof.** It suffices to check that the character values of $\bigcup_{i=1}^{l} D_{i_j}$ are as required by Lemma A. $\lambda_0(\bigcup_{i=1}^{l} D_{i_j}) = lp^{t-x}(p^t - 1)$. For any order $p$ character $\lambda_{p^m}$, $\lambda_{p^m}(\bigcup_{i=1}^{l} D_{i_j}) = -lp^{t-x}$. For any order $p^m$ character $\lambda_{(1 + ph)g^x}$, by the observation made before Theorem 3.2, we know that there is at most one $j$, $1 \leq j \leq l$, such that $\lambda_{(1 + ph)g^x}(D_{i_j}) = p^{t-x}$.

$$\lambda_{(1 + ph)g^x}(\bigcup_{i=1}^{l} D_{i_j}) = \begin{cases} p^{t-x} & \text{if } \lambda_{(1 + ph)g^x}(D_{i_j}) = p^{t-x} \text{ for some } j, 1 \leq j \leq l, \\ -lp^{t-x} & \text{otherwise}. \end{cases}$$
This shows that $D_i \cup D_{i'} \cup \cdots \cup D_{i''}$ is an $(n^2, r(n-1), n^2 + r^2 - 3r_2, r_2^2 - r_2)$-PDS in the additive group of $\text{GR}(p^2, t)$ with $n = p^t, r_2 = lp^{t-1}$. The second part of the theorem can be similarly proved. This completes the proof.

4. RELATIVE DIFFERENCE SETS

In this section, we give two constructions of relative difference sets. The first is a consequence of the construction of partial difference sets in Section 3. The second construction is for abelian 2-groups, in its general form (Theorem 4.6), the construction gives new relative difference sets in abelian 2-groups. We will maintain the notation in previous sections.

Let $G = (\text{GR}(p^2, t), +) \oplus P$, where $(\text{GR}(p^2, t), +)$ is the additive group of GR($p^2$, t), and $P$ is any abelian group of order $p^s$, where $s | t$, $1 \leq s < t$. Assume that $P = \{x_0, x_1, \ldots, x_{p^s-1}\}$. We define $R = (D_0, x_0) \cup (D_1, x_1) \cup \cdots \cup (D_{p^s-1}, x_{p^s-1}) \cup (B, 0)$, where $D_0, D_1, \ldots, D_{p^s-1}$ were defined in Section 3. Then we have the following theorem.

**Theorem 4.1.** $R$ is a $(p^{2t}, p^t, p^{2t-s})$-relative difference set in $G$ relative to $P$.

**Proof.** Let $\psi$ be an arbitrary character of $G$. Then $\psi = \lambda \otimes \chi$, where $\lambda$ is an additive character of $\text{GR}(p^2, t)$ and $\chi$ is a character of $P$. We consider two cases.

Case 1. $\chi$ is the principal character:

$$\psi(R) = \sum_{i=0}^{p^s-1} \lambda(D_i) + \lambda(B).$$

If $\lambda$ is principal, then $\psi(R) = |R| = p^{2t}$.

If $\lambda$ is not principal, then we distinguish two cases.

1. $\lambda = \lambda_{p^s}$. In this case, $\lambda$ has order $p^s$, $\lambda(B) = |B| = p^t$, and $\lambda(D_i) = p^{t-i}$, $0 \leq i \leq p^t - 1$. Hence $\psi(R) = (-p^{t-s}) p^t + p^s = 0$.

2. $\lambda = \lambda_{p^s}, \beta = (1 + pb) g^u$, where $0 \leq u \leq (q-2)$, and $b \in \mathbb{F}$. In this case, $\lambda$ has order $p^2$, $\lambda(B) = 0$, and by the observation made before Theorem 3.2, we know that there is a unique $j$, $0 \leq j \leq p^t - 1$, such that $\lambda_{p^s + pb} g^u(D_j) = p^{t-s}$. Hence $\psi(R) = p^t - p^{t-s} + (p^t - 1)(-p^{t-s}) = 0$.

Case 2. $\chi$ is nonprincipal on $P$:

$$\psi(R) = \sum_{i=0}^{p^s-1} \lambda(D_i) \chi(x_i) + \lambda(B);$$

we also distinguish three cases.
(1) \( \lambda \) is principal: \( \psi(R) = |D_0| \sum_{i=0}^{p'-1} \chi(x_i) + |B| = p' \).

(2) \( \lambda \) has order \( p \); i.e., \( \lambda = \lambda_{p^k} \). In this case, \( \lambda(B) = |B| = p' \) and
\[ \lambda(D_i) = -p^{-i} \sum_{i=0}^{p'-1} \chi(x_i) + p' = p'. \]

(3) \( \lambda \) has order \( p^2 \); i.e., \( \lambda = \lambda_{p^2} \). As in Case 1, there is a unique \( j \), \( 0 \leq j \leq p'-1 \), such that
\[ \lambda_{j+pb}(D_i) = |B| = pt \quad \text{and} \quad \lambda_{j}(D_i) = |B| = pt. \]

So we have shown that
\[
|\psi(R)| = \begin{cases} 
  pt & \text{if } \psi \text{ is principal on } G. \\
  0 & \text{if } \psi \text{ is nonprincipal on } G \text{ but principal on } P. \\
  pt & \text{if } \psi \text{ is nonprincipal on } P.
\end{cases}
\]

By Lemma B, \( R \) is a \( (p^3, pt^2, p^2, pt^{2m-1}) \)-relative difference set in \( G \) relative to \( P \). This completes the proof.

Remark. We remark that there are many constructions of \( (p^3, pt^2, p^2, pt^{2m-1}) \)-relative difference sets, see [8] for a summary. The good thing in Theorem 4.1 is that \( P \) is an arbitrary abelian \( p \)-group of order \( pt^2 \).

The RDS in Theorem 4.1 is splitting. In the following, we construct a nonsplitting RDS in abelian 2-groups.

Let \( A = \{ {\bar{x}} \in R \mid \text{tr}_x({\bar{x}}) = 0 \} \), \( G = (\text{GR}(4, t), +) \oplus (A, +) \), and \( F_a = E_a \cup \{ 0 \} \). Assume that \( A = \{ \overline{x_1}, \overline{x_2}, ..., \overline{x_{2m+1}} \} \), \( x_i \in \mathbb{F}_8 \), \( 1 \leq i \leq 2^{m+1} \). Define \( R = \{ \overline{1^{2m+1}} (F_{\overline{x_i}}, \overline{x_i}) \} \). We have the following theorem.

**Theorem 4.2.** If \( t = 2^m + 1 \), \( m \geq 1 \), then \( R \) is a \( (2^{2m+1}, 2^{2m+1}, 2^{m+1}, 2^{2m-1}) \)-relative difference set in \( G \) relative to \( B \), where \( B \) is the unique maximal ideal of \( \text{GR}(4, t) \).

**Proof.** Let \( \psi \) be an arbitrary character of \( G \). Then \( \psi = \lambda \otimes \chi \), where \( \lambda \) is an additive character of \( \text{GR}(4, t) \) and \( \chi \) is a character of \( A \).

If \( \psi \) is principal, then \( |\psi(R)| = |R| = 2^{2m+1} \).

If \( \lambda \) is principal, \( \chi \) is nonprincipal; then \( \psi(R) = |F_{\overline{x}}| \sum_{i=1}^{2^{m+1}} \chi(\overline{x_i}) = 0 \).

If \( \lambda \) has order 2, i.e., \( \lambda \) is principal on \( B \) but not principal on \( \text{GR}(4, t) \), then \( \psi(R) = \sum_{i=1}^{2^{m+1}} (1 + \lambda(E_{\overline{x_i}})) \chi(\overline{x_i}) \). Noting that \( \lambda(E_{\overline{x_i}}) = -1 \), we have \( \psi(R) = 0 \).

If \( \lambda \) has order 4, we consider two cases.

**Case 1.** \( \chi \) is principal:
\[
\psi(R) = \sum_{i=1}^{2^{m+1}} (\lambda(E_{\overline{x_i}}) + 1) = \sum_{i=1}^{2^{m+1}} \lambda(E_{\overline{x_i}}) + 2^{m+1}.
\]
By a result of Yamamoto and Yamada [9], we know that \( \sum_{i=1}^{2^{t-1}} \zeta_i E_i = \pm 2^{t-1} \xi_4 \), where \( \xi_4 = \sqrt{-1} \). Hence \( |\psi(R)| = \sqrt{2} 2^{t-1} = \sqrt{2^{2t-1}} \).

**Case 2.** \( \chi \) is nonprincipal. We assume that \( \lambda = \mathcal{L}_{1+2b} \), and \( \chi = \mathcal{X}_{g'} \), where \( g' \in H, g' \in K \), \( v \neq 0 \), then

\[
\psi(R) = \sum_{i=1}^{2^{t-1}} (\lambda E_i + 1) \chi(R)
= \sum_{i=1}^{2^{t-2}} \sum_{j=0}^{2^{t-2}} (\xi_4 T_{i+1}(1+2b) g'^{(1+2b) g'} + 1)(-1)^{\tau_i (\xi_4 g')}
= \sum_{i=1}^{2^{t-2}} \sum_{j=0}^{2^{t-2}} \xi_4 T_{i+1}(1+2b) g'^{(1+2b) g'} (-1)^{\tau_i (\xi_4 g')}
= \sum_{i=1}^{2^{t-2}} \xi_4 T_{i+1}(1+2b) g'^{(1+2b) g'} (-1)^{\tau_i (\xi_4 g')}
= \sum_{i=1}^{2^{t-2}} \xi_4 T_{i+1}(1+2b) g'^{(1+2b) g'} X_{g'}(A)
\]

Since \( A \) is the trace zero hyperplane in \( K \), if an additive character \( \chi \) is neither \( \chi_0 \) nor \( \chi_1 \), then \( \chi(A) = 0 \). Let \( g' + g'' = 0 \). Then \( g'' = g' \). If we set \( g' + g'' = 1 \), then \( g'' = 1 - g'' = g'' \) (say). Hence

\[
\psi(R) = \xi_4 T_{i+1}(1+2b) g'^{(1+2b) g'} 2^{t-1} + \xi_4 T_{i+1}(1+2b) g'^{(1+2b) g'} 2^{t-1}
= 2^{t-1}(-1)^{\tau_i (\xi_4 g') (\xi_4 g') + (-1)^{\tau_i (\xi_4 g')}}.
\]

By the commutative diagram in Section 2, we have \( \mu_i(T_{i+1}(g'')) = \text{tr}_{i+1}(g'') \), and \( \mu_i(T_{i+1}(g')) = \text{tr}_{i+1}(1 - g'') = 1 \). So if \( i \) is odd, then \( \mu_i(T_{i+1}(g'')) \) and \( \mu_i(T_{i+1}(g')) \) have opposite parity. Therefore \( |\psi(R)| = 2^{t-1} \). Summing up all these calculations, we have shown that

\[
|\psi(R)| = \begin{cases} 
2^{t-1} & \text{if } \psi \text{ is principal on } G. \\
0 & \text{if } \psi \text{ is nonprincipal on } G \text{ but principal on } B. \\
\sqrt{2^{2t-1}} & \text{if } \psi \text{ is nonprincipal on } B.
\end{cases}
\]

By Lemma B, we conclude that \( R \) is a \( (2^{4m+1}, 2^{2m+1}, 2^{4m+1}, 2^{2m}) \)-relative difference set in \( G \) relative to \( B \). This completes the proof.

**Remark.** Jungnickel [4] has given a construction of \( (2^n, 2^k, 2^n, 2^{n-k}) \)-RDS in \((\mathbb{Z}_2)^m \otimes (\mathbb{Z}_2)^{m-1}\). Our method of construction here is quite different from Jungnickel's method. Also the construction in Theorem 4.2 gives Hadamard difference sets in \((A, +)\) as we will show below, these
Hadamard difference sets in turn allow us to generalize the construction in Theorem 4.2 to more general groups.

Let $A$ and $F_a$ be the same as before, and $\lambda$ be any order 4 character of $\text{GR}(4, t)$. We assume that $\lambda = \lambda_{\gamma_1 + 2\gamma_2}$ for some $\gamma_1, \gamma_2 \in \mathcal{F}$, $\gamma_1 \neq 0$, also we will denote the trace map $T_{a,1}$ from $\text{GR}(4, t)$ to $\mathbb{Z}_4$ simply by $T$, then we have the following lemma.

**Lemma 4.1.** $\sum_{x \in \mathcal{F}} \lambda(x) = (\sum_{x \in \mathcal{F}} \xi_4^{T_{\gamma_1 + 2\gamma_2}(x)}) \xi_4^{-T_{\gamma_1}(\gamma_1)}$.

**Proof (Calderbank).** From Section E of [3], we know that $\sigma : x \mapsto (ax + b)^{2^m}$, $a, b \in \mathcal{F}$, $a \neq 0$ induces a permutation on $\mathcal{F}$. Hence

$$
\sum_{x \in \mathcal{F}} \lambda(x) = \sum_{x \in \mathcal{F}} \xi_4^{T_{\gamma_1 + 2\gamma_2}(x)} = \sum_{x \in \mathcal{F}} \xi_4^{T_{\gamma_1 + 2\gamma_2}(ax + b)^{2^m}} = \sum_{x \in \mathcal{F}} \xi_4^{T_{\gamma_1 + 2\gamma_2}(ax + b + 2(abx)^{2^m-1})} = \sum_{x \in \mathcal{F}} \xi_4^{T_{\gamma_1 + 2\gamma_2}(x + 2\gamma_2x + \gamma_1b + 2\gamma_2b + 2\gamma_1(abx)^{2^m-1})}.
$$

Noting that $T(2y) = T(2y^2)$ for $y \in \mathcal{F}$, and letting $a = 1/\gamma_1$, $b = \gamma_2/\gamma_1^2$, we have

$$
\sum_{x \in \mathcal{F}} \lambda(x) = \sum_{x \in \mathcal{F}} \xi_4^{T_{\gamma_1}(x)} = \left( \sum_{x \in \mathcal{F}} \xi_4^{T_{\gamma_1}(x)} \right) \xi_4^{-T_{\gamma_1}(\gamma_1)}.
$$

This completes the proof. 

Assume that $A = \{ \overline{x_1}, \overline{x_2}, \ldots, \overline{x_{2^t-1}} \}$, $\overline{x_1} = 0$, $x_i \in \mathcal{F}$; then $F_0 = \mathcal{F}$ and for each $i, 2 \leq i \leq 2^t-1$, $F_{x_i} = (1 + 2x_i) \mathcal{F}$. Given any order 4 character $\lambda_{1 + 2\gamma} \ast$, $\gamma \in \mathcal{F}$, $0 \leq u \leq 2^t - 2$, one has

$$
\lambda_{1 + 2\gamma} \ast (F_{x_u}) = \sum_{j=0}^{2^t-2} \xi_4^{T_{1 + 2\gamma}(1 + 2\gamma_1) \ast (1 + 2x_j \gamma^j)} + 1
$$

$$
= \sum_{j=0}^{2^t-2} \xi_4^{T_{1 + 2\gamma}(1 + 2\gamma_1) \ast (1 + 2x_j \gamma^j)} + 1
= \lambda_{1 + 2\gamma} (F_{x_u}),
$$

so we may concentrate on characters of the form $\lambda_{1 + 2\gamma}$, $\gamma \in \mathcal{F}$. 

---

**File:** 582A 271011 By:CV Date:14:15:37 Time:12:49 LOP9M. V8.0 Page 01:01

**Codes:** 2650 Signs: 1114. Length: 45 pic 0 pts, 190 mm
For any fixed \( \lambda_1 + 2\gamma, \gamma \in \mathcal{F} \), we have
\[
\hat{\lambda}_1 + 2\gamma(F_\mathcal{F}) = \sum_{x \in \mathcal{F}} \xi^T((1 + 2)\lambda_1(1 + 2\gamma)x) = \sum_{x \in \mathcal{F}} \xi^{T\beta\gamma}(1 + 2\gamma)\lambda_1 x.
\]
Assuming that \( \gamma + \lambda_1 = \beta_1 + 2\theta_1, \beta_1, \theta_1 \in \mathcal{F} \), by Lemma 4.1, we have
\[
\hat{\lambda}_1 + 2\gamma(F_\mathcal{F}) = \sum_{x \in \mathcal{F}} \xi^{T\beta\gamma}(1 + 2\beta_1 x) = \hat{\lambda}_1(F_\mathcal{F}) \xi^{T\beta\gamma}.
\]
On the other hand,
\[
\hat{\lambda}_1 + 2\gamma(F_0) = \sum_{x \in \mathcal{F}} \xi^{T\beta\gamma}(1 + 2\gamma)x = \hat{\lambda}_1(F_0) \xi^{T\beta\gamma},
\]
noting that \( \gamma^2 + 2\lambda_1 + \lambda_1^2 = \beta_1^2 \), we have
\[
\frac{\hat{\lambda}_1 + 2\gamma(F_\mathcal{F})}{\hat{\lambda}_1 + 2\gamma(F_0)} = \xi^{T\beta\gamma} = \xi^{T\beta\gamma}\gamma^2.
\]
Since \( \text{tr}(\lambda_1) = 0 \), \( T((1 + 2\gamma)\lambda_1) = T(\lambda_1) + 2T(\gamma \lambda_1) \in \{0, 2\} \).

Define \( \omega_\gamma : A \rightarrow \{\pm 1\} \) via \( \omega_\gamma(\lambda_1) = \lambda_1 + 2\gamma(F_\mathcal{F})/\hat{\lambda}_1 + 2\gamma(F_0) = \xi^{T\beta\gamma(1 + 2\gamma)} \).

We have the following theorem.

**Theorem 4.3.** If \( t = 2m + 1, m \geq 1 \), then \( \omega_\gamma^{-1}[1] \) is a \( (2^m, 2^m - 2m - 2, 2m - 2) \)-difference set in \((A, +)\) for all \( \gamma \in \mathcal{F} \).

**Proof.** First we note that
\[
\sum_{i=1}^{2^{\gamma^2}} \hat{\lambda}_1 + 2\gamma(F_\mathcal{F}) = \sum_{i=1}^{2^{\gamma^2}} \hat{\lambda}_1 + 2\gamma(E_\mathcal{F}) + 2^{\gamma^2} = 2^{2m} \pm 2^{2m} \xi_4.
\]
where \( \sum_{i=1}^{2^{\gamma^2}} \hat{\lambda}_1 + 2\gamma(E_\mathcal{F}) = \pm 2^{2m} \xi_4 \) follows from Yamamoto and Yamada [9]. Hence
\[
|\omega_\gamma^{-1}[1]| \hat{\lambda}_1 + 2\gamma(F_0) - (2^{\gamma^2} - |\omega_\gamma^{-1}[1]|) \hat{\lambda}_1 + 2\gamma(F_0) = 2^{2m} \pm 2^{2m} \xi_4.
\]
Also by a result of Boztas, Hammons, and Kumar in [1], we know that 
\[ \lambda_{1,2}(F_{\pi}) = \pm 2^n \pm 2^n \xi_4. \]
It follows that \( |\omega_0^{-1}[1]| = 2^{2m-1} \pm 2^{m-1}. \) From the proof of Theorem 4.2, Case 2, \( \chi \) is nonprincipal; therefore we have

\[
\psi(D) = \sum_{i=1}^{2^{r-1}} \lambda_{i,2}(F_{\pi}) \chi(\bar{\tau}_{i})
= \lambda_{1,2}(F_{\bar{\pi}}) \chi(\omega_0^{-1}[1]) - \lambda_{1,2}(F_{\bar{\pi}}) \chi(A \setminus \omega_0^{-1}[1])
= 2^{1,2}(F_{\bar{\pi}}) \chi(\omega_\mu^{-1}[1]),
\]
where \( \psi, \chi, \) and \( D \) are the same as those in the proof of Theorem 4.2. By Theorem 4.2, \( |\psi(D)| = \sqrt{2} \cdot 2^{2m}; \) also \( |\lambda_{1,2}(F_{\bar{\pi}})| = \sqrt{2} \cdot 2^m. \) We have \( |\chi(\omega_0^{-1}[1])| = 2^{m-1}, \) for every nonprincipal character \( \chi \) of \( A. \) Hence \( \omega_0^{-1}[1] \) is a Hadamard difference set in \( A. \) This completes the proof.

From the above theorem, we see that each \( \gamma \in F \) gives rise to a Hadamard difference set \( \omega_\mu^{-1}[1] \) in \( (A, +); \) the relationship between these \( \omega_\mu^{-1}[1], \gamma \in F, \) is given in the following proposition.

**Proposition 4.4.** (1) If \( \gamma \in F, \bar{\gamma} \in A, \) then \( \omega_0^{-1}[1] = \omega_\mu^{-1}[1] + \bar{\gamma} \) if \( T(\gamma) = 0, A \setminus \omega_\mu^{-1}[1] = \omega_0^{-1}[1] + \gamma \) if \( T(\gamma) = 2. \)

(2) If \( \gamma \in F, \bar{\gamma} \notin A, \) assuming that \( \bar{\gamma} = 1 + \pi_{x}, \) for some \( \pi_{x} \in A, \) then \( \omega_0^{-1}[1] = \omega_\mu^{-1}[1] + \pi_{x}, \) if \( T(\bar{\gamma} - 1) = 0; \) \( A \setminus \omega_\mu^{-1}[1] = \omega_0^{-1}[1] + \pi_{x}, \) if \( T(\bar{\gamma} - 1) = 2. \) Also \( \omega_0^{-1}[1] = \omega_\mu^{-1}[1]. \)

**Proof.** We prove the proposition for the case \( \gamma \in F, \bar{\gamma} \in A, T(\gamma) = 0. \) The rest of the proposition can be similarly proved.

If \( x \in \omega_0^{-1}[1], x \in F, \) then \( T(x) = 0. \) We claim that \( x + \bar{\gamma} \in \omega_0^{-1}[1], \) so \( \omega_0^{-1}[1] + \bar{\gamma} \subseteq \omega_0^{-1}[1]. \) Let \( x + \bar{\gamma} = y, y \in F. \) Assume that \( x + \bar{\gamma} = y + 2z, z \in F, \) then \( y - y = 2z - x, \) so \( y^2 - 2y\bar{\gamma} + \bar{\gamma}^2 = x^2. \)

\[
T(y(1 + 2\gamma)) = T(y^2) - 2T(\bar{\gamma}y)
= T(x^2) - T(\bar{\gamma}^2)
= -T(\bar{\gamma}) = 0.
\]

Hence \( \bar{\gamma} = x + \bar{\gamma} \in \omega_0^{-1}[1]. \) This proves the claim.

Conversely, for any \( x \in \omega_0^{-1}[1], x \in F, \) we can similarly prove that \( x - \bar{\gamma} \in \omega_0^{-1}[1]; \) hence \( x \in \omega_0^{-1}[1] + \bar{\gamma}. \)

Summing up, we have shown that \( \omega_0^{-1}[1] = \omega_\mu^{-1}[1] + \bar{\gamma} \) if \( T(\gamma) = 0. \) This completes the proof of the proposition.
We remark that \( \omega_\gamma \) can also be defined by \( \omega_\gamma (\mathcal{F}) = \xi_4^{T_1(1+2\gamma_1)x_1} \), \( x_1 \in \mathcal{F} \), since \( T_1(1+2\gamma_1)x_1 = T((1+2\gamma_1)x_1^2) \). In general, we have \( \omega_\gamma (\mathcal{F}) = \xi_4^{T_1(1+2\gamma_1)x_1^2} \), where we do not require \( x \in \mathcal{F} \). This definition is more convenient to use.

We note that \( \omega_\gamma : A \to \{ \pm 1 \} \) defines a function \( b_\gamma : A \to \{ 0, 1 \} \) via \( \omega_\gamma (\mathcal{F}) = (-1)^{b_\gamma (\mathcal{F})} \) for all \( \gamma \in \mathcal{F} \). By the relationship between Hadamard difference sets and bent functions (see [2]), we have the following corollary.

**Corollary 4.5.** \( b_\gamma \) is a bent function on \( A \cong F_{2^m} \) for every \( \gamma \in \mathcal{F} \).

We continue to study the bent functions \( b_\gamma, \gamma \in \mathcal{F} \).

**Lemma 4.2** For each \( \gamma \in \mathcal{F} \), \( b_\gamma \) is a quadratic form on \( A \cong F_{2^m} \).

**Proof.** It suffices to prove that \( b_\gamma (\mathcal{F}) - b_\gamma (\mathcal{F}) - b_\gamma (\mathcal{F}) \) is a bilinear form on \( A \). From the definition of \( b_\gamma \), we see that

\[
(-1)^{b_\gamma (\mathcal{F}) - b_\gamma (\mathcal{F}) - b_\gamma (\mathcal{F})} = \xi_4^{T_1(1+2\gamma_1)(x+y) - T_2(1+2\gamma_1)x_1^2 - T_2(1+2\gamma_1)y_1^2} = \xi_4^{T_1(2xy)} = (-1)^{tr_1(xyx)}.
\]

So \( b_\gamma (\mathcal{F}) - b_\gamma (\mathcal{F}) - b_\gamma (\mathcal{F}) = tr_1(xyx) \) is a bilinear form on \( A \). This completes the proof.

From Remark 6.3.1 of [2], we know that \( b_\gamma, \gamma \in \mathcal{F} \) (up to complementation), belong to family Q (see [2]), and it has the form

\[
b_\gamma (X, Y) = X_1 Y_1 + X_2 Y_2 + \cdots + X_m Y_m
\]

with respect to a suitable basis \( x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_m \) of \( A \) over \( F_2 \). Hence the difference set \( \omega_\gamma^{-1}[1] \) (up to complementation) is the Menon composition (which corresponds to the Kronecker product of the corresponding Hadamard matrices, see [2]) of singleton difference sets in \( Z_2 x_i + Z_2 y_i, i = 1, 2, \ldots, m \).

Let \( W = (Z_2)^r \oplus (Z_2)^s \), \( r + s = m \). We define a bijection \( f_\gamma : A \to W \) by setting \( f_\gamma = f_1^{(i_1)} \times f_2^{(i_2)} \times \cdots \times f_2^{(i_m)} \), where \( f_1^{(i)} : Z_2 x_i + Z_2 y_i \to Z_4 \) or \( (Z_2)^s \) is an arbitrary bijection. We note that the definition of \( f_\gamma \) depends on the basis \( x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_m \) of \( A \) over \( F_2 \). We need the following lemma.

**Lemma 4.3.** \( f_\gamma (\omega_\gamma^{-1}[1] + z) \) are Hadamard difference sets for all \( \gamma \in \mathcal{F} \) and \( z \in A \).

**Proof.** We prove the lemma in the case \( m = 2 \). The rest follows by induction on \( m \).
If \( m = 2 \), let \( G_i = Z_2x_i + Z_3y_i \) and let \( D_i \) be trivial difference sets in \( G_i \), \( i = 1, 2 \) (by trivial difference sets we mean that \( D_i \) is either a singleton difference set or the complement of a singleton difference set). From the discussion above we see that \( \omega_{z^{-1}}[1] = \{ D_1 \times (G_2 \setminus D_2) \} \cup \{(G_1 \setminus D_1) \times D_2 \} \).

Let \( z = (z_1, z_2) \), \( z_i \in G_i \), \( i = 1, 2 \). Then

\[
\omega_{z^{-1}}[1] + z = \{ (D_1 + z_1) \times ((G_2 \setminus D_2) + z_2) \} \cup \{(G_1 \setminus D_1 + z_1) \times (D_2 + z_2) \}.
\]

\[
f_i(\omega_{z^{-1}}[1] + z) = [f^{(1)}(D_1 + z_1) \times (f^{(2)}(G_2) \setminus f^{(2)}(D_2 + z_2))] \\
\cup [(f^{(1)}(G_1) \setminus f^{(1)}(D_1 + z_1)) \times f^{(2)}(D_2 + z_2)].
\]

Since \( D_1 \) and \( D_2 \) are trivial difference sets in \( G_1 \) and \( G_2 \), \( f^{(1)}(D_1 + z_1) \) and \( f^{(2)}(D_2 + z_2) \) are trivial difference sets in \( G_1 \) and \( G_2 \), respectively. Hence \( f_i(\omega_{z^{-1}}[1] + z) \) is a Hadamard difference set in \( f^{(1)}(G_1) \times f^{(2)}(G_2) \). The proof is complete.

With the above preparation, we can now generalize Theorem 4.2 as follows.

Let \( G = (\text{GR}(4, t), +) \otimes W \), where \( t = 2m + 1 \), \( m \geq 1 \), \( W = (Z_2)^r \otimes (Z_2 \otimes Z_2)^s \), \( r + s = m \), \( r, s \geq 0 \), and let \( f_0 \) be the bijection from \( A \) to \( W \) defined before Lemma 4.3. We define \( R = \bigcup_{d=1}^{2^{r+s}-1} (f_d(\mathcal{F})) \) where \( A = \{ \mathcal{F}, \mathcal{F}_2, \ldots, \mathcal{F}_{2^{r+s}-1} \} \), \( \mathcal{F}_0 = 0 \), \( \mathcal{F} \in \mathcal{F} \) is the trace zero hyperplane of \( K = \text{GR}(4, t)/B \). We have the following theorem.

**Theorem 4.6** \( R \) is a \( (2^{4m+1}, 2^{2m+1}, 2^{4m+1}, 2^{2m}) \)-relative difference set in \( G \) relative to \( B \), where \( B \) is the unique maximal ideal of \( \text{GR}(4, t) \).

**Proof.** Let \( \psi \) be an arbitrary character of \( G \). Then \( \psi = \lambda \otimes \chi \), where \( \lambda \) is an additive character of \( \text{GR}(4, t) \) and \( \chi \) is a character of \( W \).

If \( \psi \) is principal, then \( |\psi| = 2^{4m+1} \).

If \( \lambda \) is principal, \( \chi \) is nonprincipal, then \( \psi(\mathcal{F}) = |F_{\mathcal{F}}| \sum_{i=1}^{2^{r+s}-1} \chi(f_d(\mathcal{F})) = 0 \).

If \( \lambda \) has order 2, i.e., \( \lambda \) is principal on \( B \) but not principal on \( \text{GR}(4, t) \), then \( \psi(\mathcal{F}) = \sum_{i=1}^{2^{r+s}-1} (1 + \lambda(E_{\mathcal{F}})) \chi(f_d(\mathcal{F})) \). Noting that \( \lambda(E_{\mathcal{F}}) = -1 \), we have \( \psi(\mathcal{F}) = 0 \).

If \( \lambda \) has order 4, we consider two cases:

**Case 1.** \( \chi \) is principal:

\[
\psi(\mathcal{F}) = \sum_{i=1}^{2^{r+s}-1} (\lambda(E_{\mathcal{F}}) + 1) = 2^{r+s+1} + 2^{r+s-1} \xi_4.
\]

Hence \( |\psi(\mathcal{F})| = \sqrt{2} 2^{r+s-1} = \sqrt{2^{2r+s-1}} \).
Case 2. $\chi$ is nonprincipal. We assume that $\lambda = \lambda_{i_1 + 2\gamma}^{(\pi^*)}, \gamma \in \mathcal{T}$.

Noting that $\lambda_{i_1 + 2\gamma}^{(\pi^*)}(F_{\pi'}) = \lambda_{1 + 2\gamma}(F_{\pi'})$, we have

$$
\psi(R) = \sum_{i=1}^{2^{\gamma-1}} \lambda_{1 + 2\gamma}(F_{\pi'}) \chi(f_0(\pi')).
$$

If $\gamma = 0$, then

$$
\psi(R) = \lambda_{i_1}(F_{\pi'}) \chi(f_0(\omega_0^{-1}[1])) - \lambda_{i_1}(F_{\pi'}) \chi(W^\cap f_0(\omega_0^{-1}[1]))
= 2\lambda_{i_1}(F_{\pi'}) \chi(f_0(\omega_0^{-1}[1]))).
$$

By Lemma 4.3, we know that $|\chi(f_0(\omega_0^{-1}[1]))| = 2^{m-1}$, so $|\psi(R)| = 2\sqrt{2} 2^{m^2-1} = \sqrt{2} 2^{2m}$.

If $\gamma \neq 0$, $\pi' \in A$, then

$$
\psi(R) = \sum_{i \in A} \lambda_{i_1}(F_{\pi'}) \chi(f_0(\pi')).
$$

Let $\pi + \pi' = \pi'$. Then

$$
\psi(R) = \sum_{i \in A + \pi'} \lambda_{i_1}(F_{\pi'}) \chi(f_0(\pi' - \pi))
= \sum_{i \in A} \lambda_{i_1}(F_{\pi'}) \chi(f_0(\pi' - \pi))
= \lambda_{i_1}(F_{\pi'}) \chi(f_0(\omega_0^{-1}[1] - \pi)) - \lambda_{i_1}(F_{\pi'}) \chi(W^\cap f_0(\omega_0^{-1}[1] - \pi))
= 2\lambda_{i_1}(F_{\pi'}) \chi(f_0(\omega_0^{-1}[1] - \pi)).
$$

By Lemma 4.3, we know that $|\chi(f_0(\omega_0^{-1}[1] - \pi))| = 2^{m-1}$, so $|\psi(R)| = 2\sqrt{2} 2^{m^2-1} = \sqrt{2} 2^{2m}$.

If $\gamma = 1$, then

$$
\psi(R) = \sum_{i=1}^{2^{\gamma-1}} \lambda_{i_1}(F_{\pi'}) \chi(f_0(\pi'))
= \sum_{i=1}^{2^{\gamma-1}} \lambda_{i_1}(F_{\pi'}) \chi(f_0(\pi'))
= 2\lambda_{i_1}(F_{\pi'}) \chi(f_0(\omega_0^{-1}[1]))).
$$

Hence $|\psi(R)| = 2\sqrt{2} 2^{m^2-1} = \sqrt{2} 2^{2m}$. 

If \( \gamma \neq A, \gamma \neq 1 \), we can write \( \gamma = 1 + \beta \) with \( \beta \in A \); then \( \lambda_{1+2}(F_{\beta}) = \lambda_1(F_{\beta+1}) = \lambda_1(F_{\beta+1}) \), so

\[
\psi(R) = \sum_{\gamma \in A} \zeta_1(F_{\gamma}) \chi(f_0(\gamma))
\]

\[
= \sum_{\gamma \in A} \zeta_1(F_{\gamma}) \chi(f_0(\gamma - \beta))
\]

\[
= \sum_{\gamma \in A} \zeta_1(F_{\gamma}) \chi(f_0(\gamma - \beta))
\]

\[
= \zeta_1(F_0) \chi(f_0(\omega_0^{-1}[1] - \beta)) - \zeta_1(F_0) \chi(W \setminus f_0(\omega_0^{-1}[1] - \beta))
\]

\[
= 2\zeta_1(F_0) \chi(f_0(\omega_0^{-1}[1] - \beta)).
\]

Hence by Lemma 4.3 \( |\psi(R)| = 2\sqrt{2} 2^{m/2 - 1} = \sqrt{2} 2^m \).

In summary, we have shown that

\[
|\psi(R)| = \begin{cases} 
2^{2r-1} & \text{if } \psi \text{ is principal on } A, \\
0 & \text{if } \psi \text{ is nonprincipal on } A \text{ but principal on } B, \\
\sqrt{2^{2r-1}} & \text{if } \psi \text{ is nonprincipal on } B. 
\end{cases}
\]

Therefore \( R \) is a \((2^{4m+1}, 2^{2m+1}, 2^{4m+1}, 2^{2m}), \) relative difference set in \( G \) relative to \( B \), where \( B \) is the unique maximal ideal of \( GR(4, t) \).

**Remark.** If we replace the group \( W \) in Theorem 4.6 by any abelian 2-group \( L \), and if there is a bijection \( \rho: A \rightarrow L \) which maps every translate of \( \omega_0^{-1}[1] \) to a difference set in \( L \), then the construction in Theorem 4.6 still works for the group \((GR(4, t), +) \oplus L \), but it seems difficult to construct such a bijection \( \rho \) except in the case \( W = (Z_4)^r \oplus (Z_2 \oplus Z_2)^s \), \( r + s = m, r, s \geq 0 \).

**ACKNOWLEDGMENTS**

The authors thank Dr. A. R. Calderbank for his generous help, in particular, the third author thanks Dr. A. R. Calderbank for kindly showing him the proof of Lemma 4.1 which is very important in understanding the Hadamard difference sets \( \omega_0^{-1}[1] \). Finally, the first author thanks Professor Henry Glover for his guidance and encouragement.

**REFERENCES**
